Customer Department TCP/IP Access to State Controller's Office Applications

May 27, 2003

California Health and Human Services Agency Data Center
Customer Department TCP/IP Access to State Controller's Office Applications

Table of Contents

1 - SCO TCP/IP Access

Customers of HHSDC routed network services are able to request access to State Controller's Office (SCO) applications via their LAN-attached workstations and printers that are connected to the HHSDC wide area network.

This document outlines the basic steps that the customer department needs to take, provides an explanation of TCP/IP terminal and printer access of SCO applications and details the information needed for the HHSDC service request.

Note: The customer department must contact the State Controller's Office directly for information about SCO's specific requirements.

Outline of the Steps for Requesting Access

The basic steps for requesting access include:

1. Contact the State Controller's Office to obtain SCO's requirements for granting TCP/IP access.

   Note: Reviewing the SCO Security Memorandum in Appendix C will provide the customer department with insight on the information that SCO will require from them. The HHSDC has a response on file with SCO for the relevant items of the Security Memorandum.

2. Install TN3270 software on IP defined workstations (if not already installed)

3. Submit the HHSDC service request for TCP/IP access to SCO through your department's HHSDC service request coordinator

4. HHSDC creates and returns VTAM terminal and printer definitions to the customer department

5. Submit the request to SCO for TCP/IP access through your department's SCO contact person

2 - Departmental Contacts

Before requesting access, you should identify who your contacts are, within your department, for submitting SCO and HHSDC requests. As part of the request process, you should communicate with SCO and HHSDC through these designated contacts.

SCO Departmental Contact

Your SCO Departmental Contact is the person in your department authorized to submit requests and communicate with SCO.

Each State department's payroll section has an assigned SCO Departmental Contact. If you do not know your SCO Departmental Contact, you can contact:

For Personnel/Payroll (PPSD) services:

State Controller's Office
Personnel/Payroll Services Division
P. O. Box 942850
Sacramento, CA 94250-5878.
Attn: Information Security Administrator

You may also contact the PPSD Administrator @ (916) 324-5879.

For Accounting and Reporting Financial Systems (DAR) services:

State Controller's Office
Division of Accounting and Reporting
P. O. Box 942850
Sacramento, CA 94250-5878.
Attn: Information Security Administrator

You may also contact the DAR Administrator @ (916) 324-2341

HHSDC Service Request Coordinator

Your HHSDC Service Request Coordinator is the person in your department who has access to the HHSDC service request (SR) system and is able to create and submit HHSDC SRs.

If your department does not currently have an HHSDC Service Request Coordinator, please contact your HHSDC Customer Relations Representative. Your HHSDC Customer Relations Representative will work with you to set someone up as an HHSDC service request coordinator.

If you do not know who your HHSDC Customer Relations Representative is, please contact the HHSDC Customer Relations Unit at 454-7225.

3 - Terminal (Workstation) and Printer Connectivity

Customer department's workstations and printers requiring access to SCO must be attached to a LAN that is connected to the HHSDC wide area network. The workstations and printers must be configured by the customer with IP addresses from an HHSDC IP address subnet range.

As part of the HHSDC service request, the customer must identify the staff person, the workstations and printers requiring SCO access, the IP addresses and the IP address subnet range that the equipment is configured with.

How Terminal (Workstation) Access Works

(Please refer to Appendix A – Definitions, for an explanation of various terms and acronyms)

The customer's workstations will use TN3270 emulation software configured for 3270 Model 2 terminals.

Note: The customer department is responsible for providing, installing and maintaining the TN3270 emulation software.

HHSDC will make TN3270 server and VTAM definitions that associate the customer's workstations IP addresses to a pool of VTAM LUNAMEs.

The list of the staff people requesting access, workstation's IP addresses, the pool of associated LUNAMEs are information that SCO will most likely ask for as part of the SCO request (please refer to SCO for their request requirements).

How Printer Access Works

(Please refer to Appendix A – Definitions, for an explanation of various terms and acronyms)

The three components of TCP/IP printing for SCO applications are part of the HHSDC mainframe system:

1 - DRS (Dynamic Reporting System)
2 - JES (Job Entry Subsystem) Spool
3 - VPS (VTAM Print System)

DRS simulates VTAM printers. Output is sent to DRS by specifying a certain VTAM APPLID (SCO regards these APPLIDs as the printer's LUNAMEs).

Output sent to DRS is stored in the JES Spool disk file until it is printed out. The JES Spool is managed by JES. Items in JES Spool can be accessed via two programs, IOF (Interactive Output Facility) and VMCF (VPS Monitor and Control Facility).

> Note: IOF is the program that monitors IBM mainframe host batch jobs and allows control of output. VMCF is the menu-driven control interface to VPS and is used to monitor VPS-controlled output devices.

Description of SCO Application Printing

The following describes how print output is generated in an SCO CICS application and then is sent to a customer's LAN-attached, TCP/IP-defined printer:

- An SCO CICS application generates print output and directs it to a CICS terminal ID that is associated to a VTAM APPLID/LUNAME (specific printer identification in VTAM)
- Print output sent to that APPLID/LUNAME is given to DRS
- DRS moves the print output to a SYSOUT dataset in JES Spool and associates that print output to a printer's U number via the APPLID/LUNAME
- VPS scans JES Spool, finds the print output and resolves the destination of the print output to the IP address of a specific printer via its U number
- VPS sends the print output from JES Spool to that printer
- VPS tells JES to purge the print output dataset

Printer Security

There are several security aspects to be considered in print access. These are:

- Access to unprinted output datasets
- Modification of printer TCP/IP addresses
- Modification of DRS and VPS printer definitions
- Access to unprinted output datasets

Access to unprinted datasets is controlled as follows:

A special RACF profile will be created that prevents anyone from viewing the DRS SYSOUT datasets. The JES log, JCL listing and MVS logs will be accessible for troubleshooting only by HHSDC technical staff.

VPS Security – VPS utilizes its own security procedure. Each printer is associated with a group of users via the user's MVS RACF IDs. Each user within the group is granted specific access.

For SCO connected printers, special groups will be set up. These groups will be named SCOxxx, where xxx is unique to the customer department. Within the security table, a default profile will be set up which allows only the HHSDC Online Support Unit to alter the TCP/IP address of a printer associated with an SCOxxx group.

The security table default profile will also prevent unauthorized staff from using VMCF to view or to requeue the output for SCO printers.

A specific profile will also be set up for each SCOxxx group to give that customer department's Help Desk personnel and the HHSDC Help Desk personnel the ability to manipulate the printer.

Note: HHSDC Help Desk personnel will not be able to view the contents of the queued output for these printers.

- Modification of printer IP addresses

The default profile for groups whose names begin with the letters SCO will be set up to prohibit anyone other than authorized staff from performing the command to alter an IP address.

Note: Changes made to a printer's IP address by this method would only apply until the printer definition is next activated, which is typically done weekly.

- Modifying DRS and VPS printer definitions

  HHSDC Online Support Unit staff are the only ones authorized to modify DRS and VPS source printer definitions. Source printer definitions are used when the printer is activated, normally at the startup of the VPS task.

  DRS and VPS printer definitions for SCO printing will be highlighted as such. Changes to the IP address or queue name for these printers will only be made when requested through an HHSDC Service Request.

4 - HHSDC SCO TCP/IP Access Service Request

This section details what is needed for the HHSDC service request.

Information Required for the HHSDC Service Request

(Refer to Appendix B - Worksheet - HHSDC SCO TCP/IP Access Service Request).

Prepare and submit the HHSDC SCO TCP/IP Access service request. Once the SR has been received and processed, it will be routed to the proper units: the HHSDC Network Software Support group will create the terminal definitions and the HHSDC CICS group will create the printer definitions. The definitions will become active at the next mainframe system restart (IPL) which typically falls on the first and third Mondays of each month.

When the required information has been gathered, the service request should be created and submitted by your departmental HHSDC service request coordinator.

Include the following information in the service request:

Staff Terminal Access Information

- The staff requesting terminal access to SCO applications
- The IP address subnet of each staff person's workstation (terminal) to be used for access to SCO applications

Staff Printer Access Information

- The staff requesting print access to SCO applications and their HHSDC MVS RACF IDs
- Printer information (required for each printer to be used to print SCO application data):

  If the printer already has a U number, but no APPL defined, then provide the U number

  Otherwise, provide the following information for each printer:

  Printer's IP address
  Queue name, if any
  Does the printer support PCL?

Note: Each terminal and printer entry must also include the SCO application(s) to be accessed.

VTAM Information Returned on the Completed Service Request

When HHSDC completes the service request, VTAM information and equipment configuration information will be entered into the comment field of the SR and routed back to the requesting customer department.

VTAM information returned on the completed HHSDC SR:

- Terminal LUNAMEs
- Printer APPLIDs and U numbers

The completed HHSDC SR will provide for audit trail documentation.

Customers will need to include the appropriate terminal and printer VTAM information in the request they send to SCO (please refer to SCO for their request requirements).

Appendix A

Definitions

APPL / APPLID
(APPLication program IDentification) is the symbolic name of a logical unit (LU) in a VTAM network.

CICS
(Customer Information Control System) is an IBM licensed on-line transaction processing system capable of supporting a network of many terminals.

CICS Terminal ID
A CICS identifier that is associated with a VTAM LUNAME (see ‘LUNAME’).

DRS
(Dynamic Report System) lets you dynamically route output created by your online applications to the JES spool. From the JES spool, you can then direct print jobs to TCP/IP printers, VTAM printers, and LAN printers.

IOF
(Interactive Output Facility) the program that monitors IBM mainframe host batch jobs and allows control of output.

IP Address Subnet
The range of IP addresses contained in a particular subnet (see ‘subnet’).

JES
(Job Entry Subsystem) is a subsystem of the OS/390 and MVS mainframe operating systems that manages jobs (units of work) that the system does. Each job is described to the operating system in job control language (JCL). The operating system sends the job to the JES program. The JES program receives the job, performs the job based on priority, and then purges the job from the system.

JES Spool
Refers to the queue (disk file) that output from JES is held in until it is printed out. The JES Spool is managed by JES. Items in JES Spool can be accessed via two programs, IOF (Interactive Output Facility) and VMCF (VPS Monitor and Control Facility).

LUNAME
(Logical Unit NAME) is the identification name of a network accessible device (terminal or printer) in a VTAM network.

PCL
(Printer Command Language) controls a range of printer features across a number of printing devices. PCL was developed and used by Hewlett-Packard and has become a standard for control of laser and inkjet printers.

RACF
Resource Access Control Facility is the IBM security management product used in its mainframe environment. It is an IBM licensed program that provides for access control by identifying and verifying users to the system, authorizing access to protected resources, logging detected unauthorized attempts to enter the system, and logging detected accesses to protected resources.

Subnet
An extension of the IP addressing scheme that allows a site to divide a single IP network address into multiple physical networks called subnets (sub-networks).

TN3270
An extension of the Telnet protocol that allows communication with IBM host machines.

TN3270 Server
A host device running a TN3270 server application. A TN3270 server provides a translation between the TN3270 protocols used by the client emulator and the protocols used by the SNA-based application.

UID / U Number
(User ID Number) uniquely identifies a user (printer) to the system.

VMCF
(VPS Monitor and Control Facility) is a full-screen, menu-driven interface to VPS. This interface can be used to monitor all VPS-controlled output devices. VMCF gives you a single point of control for network printing, giving you and your users the means to identify problems, and do something about them.

VPS
(VTAM Printer Support) provides the ability to route JES2 spooled output to VTAM or TCP/IP printers. Through JES2 special routing and the VPS subsystem, print can be routed to 3270-type printer (VTAM) and network connected printers (TCP/IP).

VTAM
(Virtual Telecommunications Access Method) is a communications access method that uses SNA protocols for sending/receiving data. A set of programs that control communication across a network between terminals and application programs.

Appendix B

Worksheet - HHSDC SCO TCP/IP Access Service Request

Provide the following information in the HHSDC service request:

Staff Terminal Access Information

- A list of staff people requesting access to SCO applications, their workstation's IP address and the SCO application(s) that will be accessed

  (Example List)

  _____ (Staff Person)

  _____ (Workstation IP Address Subnet)

  accessing SCO application(s) _____ (application)

  _____ (application)

  _____ (application)

Staff Printer Access Information

- A list of printer information (required for each printer to be used to print SCO application data):

  Name of staff to use this printer
  Staff's HHSDC MVS RACF ID

  If the printer already has a U number, but no APPL defined, then please provide the U number

  Otherwise, provide the following information:

  Printer's IP Address
  Queue Name, if any
  Does the printer support PCL?

(Example of the Printer List for printers <u>with</u> assigned U numbers)

_____ (Staff) _____ (HHSDC MVS RACF ID)

_____ (Staff) _____ (HHSDC MVS RACF ID)

_____ (Staff) _____ (HHSDC MVS RACF ID)

using printer _____ (Printer U Number)

to print SCO application(s) _____ (application)

_____ (application)

_____ (application)

(Example of the Printer List for printers without an assigned U number)

_____ (Staff) _____ (HHSDC MVS RACF ID)

_____ (Staff) _____ (HHSDC MVS RACF ID)

_____ (Staff) _____ (HHSDC MVS RACF ID)

using printer

Printer's IP Address _____

Queue name, if any _____

Does the printer support PCL? _____

to print SCO application(s) _____ (application)

_____ (application)

_____ (application)

Appendix C

SCO Security Memorandum

Following is an SCO memorandum that addresses their security requirements for decentralized client access. Reviewing this memorandum will provide insight for the type of information SCO requires.

SCO TELEPROCESSING SECURITY REQUIREMENTS EQUIPMENT AND SYSTEM ACCESS

All requests for teleprocessing/equipment connection and access (i.e., LANs, personal computers, terminals, printers, etc.) into the SCO mainframe hosted at the Teale Data Center must be made in writing by the authorizing business manager of the specific function (i.e., Personnel, Payroll, Accounting or Human Resources) and submitted to the appropriate Controller's Office Business Program Security Administrator (Personnel/Payroll, Accounting).

It should also be noted that the equipment and system review process involves several organizations and as such, takes considerable time to complete. The State Controller's Office will make every effort to meet our clients' deadlines however; ample lead-time is essential if critical deadlines are to be met.

The following is a list of information required to accurately ascertain the security ramifications of your access. Your agency's computing configuration and security measures must be included in your request when applicable:

1. Purpose of the request; such as: new system access, system merger, adding and/or changing type of equipment (i.e., terminals, personal computers (PCs), printers, etc.); office relocations; connecting standalone PCs to a Local/Wide Area Network (LAN/WAN); or changing network communications protocols etc.

2. Identify the number of devices (i.e., three workstations and one printer, two PCs and two laser printers, replacing five dumb terminals with LAN connected PCs, etc.).

Proposals involving major changes such as the elimination of 3270 cluster controllers and / or dumb terminals in favor of LAN based connectivity technologies must include the following information:

1. A detailed network schematic showing the complete connectivity from user workstation to Teale Data Center and any other connectivity to public (Internet) as well as all other private networks.

2. A description of how terminal emulation will be achieved.

3. What is the policy and all related procedures that assure the security of key network components such as servers, routers, hubs, etc?

4. User Authentication

   a. How are network users authenticated?
   b. What are the userid and password rules regarding length of password, frequency of password change, number of grace logins, and number of invalid attempts?
   c. What happens if the user exceeds the maximum number of password attempts?
   d. Can passwords be recycled?
   e. What is the procedure to request a network userid?
   f. Are there controls in procedures to ensure only authorized requests are processed?
   g. What is the defined procedure for deleting obsolete userids in a timely manner?
   h. What is the procedure for a user to request a password reset? Describe the procedures that ensures the requester is the owner of the userid?
   d. Who has access to Administrator accounts on the network? (Servers, Network Administration and Desktops)
   e. Are there policies or procedures that prohibit the storing of userids, passwords or automated login functions on workstations?

5. Unattended Active Sessions

   a. Unattended sessions are opportunities for unauthorized update or access of data. What automated security controls are used on the network or individual workstations to protect sensitive or confidential data during unattended active sessions?

6. Enterprise Access Controls

   a. How are users restricted to only their authorized data?
   b. What is the procedure for requesting access to additional network resources after establishment of the userid?
   c. What is the procedure for removing access to network resources?
   d. Have the built-in Administrator and Guest userids been deactivated or renamed?

7. Logging, Reporting, Alerting, and Auditing

   a. Are all accesses and attempted accesses logged to a file or database?
   b. If no, what type of audit trail is being generated and can be generated?

8. Security Incidents

   a. All security incidents are to be reported to the Agencies' ISO. What is the procedure for handling and reporting an intrusion or unauthorized access to the network?

9. Security Patch Management

   a. Describe the policies and related procedures used to maintain the server and desktop computing environments with the most recent vendor-supplied critical security updates that mitigate published security exposures.

10. Virus Protection

   a. Describe the policies and related procedures to protect your organization from a computer virus attack. The description must include the procedure for protecting the networking environment from viruses, how workstation and servers are identified after being infected and reporting a virus infection once detected.

11. Security Countermeasures

   a. Describe any additional security related countermeasures in use but not addressed by this survey.

12. Remote Access to Network

   a. Describe all remote access that is in use and how remote users are authenticated.
   b. What are the procedures for requesting remote access to the network?
   c. Describe the hardware/software required for remote access connectivity and how they are administered.
   d. If this request is for the purpose of access to the Human Resource system (Personnel/Payroll), describe how remote access will be implemented to prohibit access to the H/R Systems remotely.
   e. What are controls implemented to restrict dial-in/out traffic to servers?

13. Internet Access

a. What Internet services are available?
b. What is the process for requesting and adding new services?
b. What is the procedure for requesting Internet access?
c. What policies and procedures are in place that restricts access into the network from the Internet?
d. Describe the firewall(s) rules in use.
e. Who administers the rules placed on firewalls?
f. Who administers routers?

. If SNA architecture is to be used either through 3270 cluster controllers or LAN based gateways, provide the device netname/VTAM ID numbers (PC, terminal, printer), please list the following:

- Cluster ID Number
- Terminal/PC ID Number (Netname/VTAM) and Model Type
- Printer ID Number (Netname/VTAM) and Model Type

For All Requests Please Provide

. Names and phone numbers of project staff involved:

a. Agency's Data Processing or technical staff
b. Agency's TEALE/HHSDC Client Representative
c. Agency's TEALE/HHSDC Network Planner

For requests for service regarding equipment and/or system changes connecting to the Personnel/Payroll (PPSD) services must be sent to the:

State Controller's Office
Personnel/Payroll Services Division
P. O. Box 942850
Sacramento, CA 94250-5878.
Attn: Information Security Administrator

You may also contact the PPSD Administrator @ (916) 324-5879.

For requests for service regarding equipment and/or system changes connecting to the Accounting and Reporting Financial Systems (DAR) services must be sent to the:

State Controller's Office
Division of Accounting and Reporting
P. O. Box 942850
Sacramento, CA 94250-5878.
Attn: Information Security Administrator

You may also contact the DAR Administrator @ (916) 324-2341

PLEASE NOTE: Requests to order and/or lease equipment should be directed to either your Departmental Data Processing/Computer Services Office (whoever provides this service for all your other computer needs) or your Data Center client representative (TEALE, HHSDC, etc.). It cannot be stressed enough that sufficient lead-time is necessary for the State Controller's Office to review/approval process. Please consider this to avoid delays.